REMARKS

Claims 1-12, 14-23, and 25-29 remain pending in this application. Claims 1, 26, and 29 are independent claims. The pending claims stand rejected. The assignee traverses the rejections of the pending claims.

Claim 13 has been canceled herein because the subject matter of claim 13 has been moved to the independent claims in order to further clarify the subject matter being claimed. Because the amendments to the independent claims are based upon the pre-existing subject matter of claim 13, a final office action on any subsequently newly cited art would be premature.

Claim Rejections - 35 U.S.C. § 103

Claims 1-2, 5-23, 25-28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application No. 2003/0115448, application of Bouchard (Bouchard) in view of U.S. Patent Application No. 2002/0065042, application of Picoult et al. (Picoult). Claims 3-4 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Bouchard in view of Picoult, and further in view of U.S. Patent No. 6,795,924, issued to Kiessling et al. (Kiessling). These rejections are traversed.

Claim 1 is directed to a method for handling secure message attachments for a mobile device wherein a secure message is processed at a server in order to locate a second attachment within the secure message. As amended with the subject matter of dependent claim 13, claim 1 recites that the secure message without the second attachment is sent to the mobile device. Claim 1 further recites that a request is received for the second attachment from the mobile device and that the second attachment is then provided to the mobile device. As support for these features, the specification of the instant application at page 13, lines 9-15 provides:

> Because the mobile device 100 is typically resource-limited and in order to save bandwidth, the message server 106 may elect not to initially send the attachment 102 to the mobile device 100 over a wireless connector system 108. While viewing the message on the mobile device 100, a user can request that the message's associated attachment data 102 be transmitted to the mobile device 100 over the wireless connector system 108. It is noted that the wireless connector system 108 may include a wireless network, wireless gateway, and/or wide area network.

Thus, the message server, under the method recited in claim 1, can send the attachment to the mobile device, independent of the sending of the original message within which the second attachment was located. With this capability, the message server can reduce the burden on wireless networks by avoiding the potentially unnecessary transmission of attachments, which can be quite large. Such a method also can save the users of the mobile devices within the network from bearing the monetary costs associated with downloading unnecessary data to the mobile device, and it can improve the perceived response time for message retrieval using a mobile device. (It should be understood that such a message server, as amended under the method of claim 1, is required to have the functionality of providing the secure message to the mobile device without the second attachment to the mobile device, but is not precluded from having other optional operational capability in handling a secure message, such as having the operational capability of being able to send a secure message with attachments to the mobile device.)

Page 5 of the office action maintains that such subject matter (that was originally in dependent claim 13) is disclosed in Picoult. More specifically, the office action cites to paragraph 31 of Picoult and further adds that "there might be a rule from the recipient, determining how the second attachment is handled." Paragraph 31 of Picoult is as follows:

> [0031] The method flow chart continues at step 260 where data center 120 sends to recipient's determined preferred mobile device 130 a message and any attachments. The message may be sent directly, automatically, and in accordance with a predetermined sent [sic] of criteria or upon the user

> prompting the request. At step 270, recipient selects on mobile device 130 which message recipient desires to receive. At step 280, the recipient may be queried as to whether or not the recipient would like the message to be sent securely. If the answer to the query at step 280 is "no", then the method progresses directly along path A. If, however, the answer to the query at step 280 is "yes," then the method proceeds to step 290 where the message is processed for secure transmission. Secure transmission may be effected in a variety of methods such as by public key, private key encryption, or the like. Such security techniques are well-known in the art of secure messaging; therefore, a detailed description of these secure transfer technologies is not required for an understanding of this invention. The method then progresses from step 290 to continue along path A.

This passage from Picoult teaches that a message and any attachments are sent to a recipient's preferred mobile device. The sending of the message and any attachments can be directly sent to the preferred mobile device based upon a set of criteria. However, there is no disclosure in this cited passage of Picoult that the secure message without the second attachment is sent to the mobile device and further that a request is received for the second attachment from the mobile device in order for the second attachment to be provided to the mobile device as required in claim 1. The office action appears to agree with this, but adds that "there might be a rule from the recipient, determining how the second attachment is handled." It appears that the office action is taking notice that there might be inherent in Picoult a rule for providing to a mobile device a secure message without the second attachment and later providing the second attachment to the mobile device upon receiving a subsequent request for the second attachment from the mobile device. However, a mere statement that such a specific rule ***might*** be known is insufficient for a finding of obviousness. The fact that rules in general are known does not logically lead to the conclusion that it is obvious that there might be a specific rule for providing to a mobile device a secure message without the second attachment and later providing the second attachment to the mobile device upon receiving a subsequent request for the second attachment from the mobile device. Without a specific showing as to why such a specific rule is

known and is obvious, the rejection of claim 1 under 35 U.S.C. § 103(a) is insufficient. The MPEP addresses the inappropriateness of this type of rejection in § 2112 (IV) which states (emphasis added):

> The fact that a certain result or characteristic ***may*** occur or be present in the prior art is ***not sufficient*** to establish the inherency of that result or characteristic. In re Rijckaert, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (reversed rejection because inherency was based on what would result due to optimization of conditions, not what was necessarily present in the prior art); In re Oelrich, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.' " In re Robertson, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (citations omitted) (The claims were drawn to a disposable diaper having three fastening elements. The reference disclosed two fastening elements that could perform the same function as the three fastening elements in the claims. The court construed the claims to require three separate elements and held that the reference did not disclose a separate third fastening element, either expressly or inherently.). >Also, "[a]n invitation to investigate is not an inherent disclosure" where a prior art reference "discloses no more than a broad genus of potential applications of its discoveries." Metabolite Labs., Inc. v. Lab. Corp. of Am. Holdings, 370 F.3d 1354, 1367, 71 USPQ2d 1081, 1091 (Fed. Cir. 2004) (explaining that "[a] prior art reference that discloses a genus still does not inherently disclose all species within that broad category" but must be examined to see if a disclosure of the claimed species has been made or whether the prior art reference merely invites further experimentation to find the species.

In view of the above, the basis for the rejection of this subject matter of claim 1 from claim 13 is insufficient to render the claim obvious. Accordingly, it is respectfully requested that the rejection of claim 1 be withdrawn and that claim 1 proceed to issuance.

Assignee disagrees with other positions in the office action, such as with respect to dependent claim 14. Claim 14 recites that a user request results in the second attachment being provided to the mobile device. As discussed above, the second attachment (which is provided based upon a request from the user of the mobile device) is sent at a different time than the secure message. This feature makes it possible to avoid unnecessarily downloading the data of

the second attachment and incurring the associated charges and delays. In rejecting claim 14, the office action cites to paragraph 31 of Picoult (which is the same paragraph from Picoult as discussed above) as disclosing the subject matter recited in claim 14. However, there is no disclosure in Picoult of the specific subject matter in claim 14 – that is, a user request (e.g., from the user of the mobile device) separately requesting that the second attachment be provided to the mobile device. Similar to the discussion above, the office action appears to agree with this, but adds that "there might be a rule from the recipient, determining how the second attachment is handled." However, this basis for rejecting claim 14 is insufficient since the fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. (See, *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993)) Because of the insufficiency of the basis for the rejection, claim 14 is allowable and should proceed to issuance.

As another example, assignee also respectfully disagrees with the rejection of dependent claim 19. Claim 19 recites that the second attachment is automatically provided by the server to the mobile device when the secure message is opened by the mobile device's user. Especially when viewed in context of the subject that was added to claim 1, claim 19 requires that when a secure message (which had been sent without the second attachment to the mobile device) is opened by the mobile device's user, the server then operates to automatically send the second attachment to the mobile device. In rejecting claim 19, the office action cites to paragraphs 62 and 63 of Bouchard, which read as follows:

> [0062] If the satellite e-mail server 212 cannot receive messages from the master e-mail server 224, then the satellite e-mail server 212 discards any received message (STEP 708). If, however, the satellite e-mail server 212 determines that it can receive messages from the second organization's master e-mail server 224, the satellite e-mail server 212 decrypts the second encrypted e-mail 540 (STEP 712). Because the master e-mail

> server 224 encrypted the third e-mail 532 using the first organization's public key, the satellite e-mail server 224 decrypts the second encrypted e-mail 540 using its private key. Therefore, assuming that the private key of the satellite e-mail server 224 is secure and confidential (i.e., only the satellite e-mail server 224 "knows" the private key), the second encrypted e-mail 540 can only be decrypted by the satellite e-mail server 224. The server 212 then extracts the first encrypted e-mail 524 and transmits the e-mail 524 to the first organization's corporate e-mail server 216 over the main client-router communication channel 146 and the second client-router communication channel 143 (shown with arrow 258 in FIG. 2). The corporate e-mail server 216 performs its normal operations when receiving the first encrypted e-mail 524, such as scanning for viruses. The corporate e-mail server 216 then examines the recipient address of the first encrypted e-mail 524 and subsequently delivers the e-mail 524 to the user operating the desktop 220 over the main client-router communication channel 146 and the third client-router communication channel 144 (shown with arrow 262 in FIG. 2) (STEP 716).
>
> [0063] The desktop 220 receives the first encrypted e-mail 524. The desktop 220 then verifies the digital signature of the first encrypted e-mail 524. Because the master e-mail server 224 encrypted the second e-mail 508 with the second organization's private key, the desktop 220 needs the second organization's public key to decrypt the first encrypted e-mail 524. This key is public and typically available to anyone. Therefore, the desktop 220 obtains the public key of the second organization and uses this public key to extract the second e-mail 508 from the first encrypted e-mail 524.

These passages from Bouchard teach that a desktop receives an encrypted e-mail that contains a second encrypted e-mail, and then allows the desktop to extract the second e-mail from the first encrypted e-mail. In contrast to the subject matter recited in claim 19, there is no disclosure in these passages from Bouchard of a second attachment being automatically provided by a server to mobile device in response to a secure message being opened by the mobile device is user. Instead, Bouchard discloses the desktop having the e-mail content without any additional transmission from the server being needed or being in response to a prior opening of a secure message as required by claim 19. Because of such differences between Bouchard (whether considered alone or in combination with the other cited references) and claim 19, claim 19 is patentable and should proceed to issuance.

Independent claims 26 and 29 have been amended with subject matter analogous to that added to claim 1. Thus, for at least the reasons set forth herein with respect to claim 1, claims 26 and 29 also are allowable and should proceed to issuance.

Because independent claims 1, 26, and 29 are allowable, their respective dependent claims also are allowable and should proceed to issuance. It is noted that the assignee has not, at this time, presented arguments with respect to certain dependent claims in the instant application. The assignee nevertheless reserves the right to argue the patentability of all of the dependent claims in the instant application at a future time, should that become necessary.

CONCLUSION

For the foregoing reasons, assignee respectfully submits that the pending claims are allowable. Therefore, the examiner is respectfully requested to pass this case to issuance.

Respectfully submitted,

By: _____

John V. Biernacki
Reg. No. 40,511
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, Ohio 44114
(216) 586-3939